CHAPTER I: POLICY AND PROGRAM MANAGEMENT

Section 2 - Program Management: Add the following:

1-201a (added). The Commander in Chief, HQ USEUCOM, has designated the Special Assistant for Security Matters (ECSM) as the Senior Information Security Authority for HQ USEUCOM and its assigned Elements.

1-201c (added). Directors, ODC Chiefs, Chiefs of Special Staff Offices, and Direct Reporting Units will appoint a unit level Security Manager(s) to manage and oversee organizations' Information Security Program. Security Mangers should hold the rank of E-5/GS-05 or above, have required security clearance for the level of material handled/retained by the unit, and have direct access to the director/commander. Appointed Security Managers must attend a formal HQ USEUCOM Security Managers Training Course prior to, or within the first six months of appointment. Send a copy of appointment letter to ECSM-SP. Duties performed by unit level security managers will include:

a. Conduct semiannual self-inspections of their elements. Results will be maintained on file for one year.

b. Conduct and document indoctrination and recurring training and briefing requirements in accordance with chapter IX.

c. Develop a Standard Operating Procedure pertaining to the security operations of their particular element. Organizations assigned to Hq USEUCOM at Patch Barracks will use the "HQ USEUCOM Information Security Operating Instruction". Directorate/Staff Office specific instructions should be developed to supplement this instruction.

d. Maintain a continuity notebook which includes, but is not limited to the following:

1. Security Manager, NATO Control Point, Physical Security Officer, and Top Secret Control Officer Letters of Appointment.

2. Area and/or Office Standard Operating Procedures or Memorandums referring to Security Procedures and Policies.

3. Documentation of Training and Briefings.

4. DOD 5200.1-R, Information Security Program Regulation as supplemented.

1-202 (added). The Special Assistant for Security Matters will designate in writing a properly cleared, professional commissioned officer (0-3 or above), warrant officer, or DA civilian in the 080-series, whose job is classified at grade GS-12 or above, as security manager. The HQ USEUCOM Security Manager will do the following:

a. Advise and represent the Special Assistant for Security Matters on issues relating to classification, downgrading, declassification, amd safeguarding of national security information.

b. Provide technical guidance and assistance to element security managers.

c. Establish, implement, and maintain an effective security education program. Ensure that security education requirements outlined in Chapter IX are complied with.

d. Conduct staff assistance oversight reviews of component, HQ USEUCOM staff, and field element information security

programs.

e. Assist in the training of Information Security Managers.

TABLE OF CONTENTS

CHAPTER I

GENERAL PROVISIONS

Page xiv, Appendices. Add the following titles to the Appendix List.

Appendix F .... Original Secret Classification Authorities
Appendix G .... Classified Material Destruction Standards
Appendix H .... Eastern European and Specified Countries
Appendix I .... Sample Preliminary Inquiry Report Memorandum
Appendix J .... Sample Courier Authorization Memorandum and
Exception to Policy
Appendix K .... Open Storage Request Procedures

Page I-1, paragraph 1-100, References. Add the following:

USSAN 1-69, "United States Implementation of NATO Security Procedures," 1982.

Page I-5, paragraph 1-205, Sensitive Compartmented and Communications Security Information. Add the following:

ECJ2-SSO will provide guidance on security, use, and dissemination of Sensitive Compartmented Information (SCI)

material in accordance with applicable directives. ECJ6 will provide guidance on security, use, and dissemination of Communications Security Information (COMSEC and COMPUSEC).

Page I-10, Definitions. Add the following definitions:

1-338 Security Deviation: An incident that involves the misuse or improper handling of classified material but does not fall in the categories of compromise or probable/probable compromise.

1-339 Open Storage: Storage of classified material outside of a GSA approved security container.

Page I-12, paragraph 1-600b, Delegation of Classification Authority. Add the following to the subparagraph:

b. Within USEUCOM, the Commander in Chief, Deputy Commander in Chief, and Chief of Staff have Top Secret Original Classification Authority (OCA). HQ USEUCOM elements delegated Secret and Confidential classification authority are listed at Appendix F.

Page I-13, paragraph 1-600d, Training Requirements for OCA. Add the following to the subparagraph:

d. A videocassette production titled, "Classification Management: A Decision Making Process" satisfies the indoctrination discussed in paragraph 1-600d.

Page I-14, paragraph 1-601, Derivative Classification Responsibility. Add the following subparagraph:

d. Derivative classifiers should challenge the classification of information when they have substantial reason to believe that information is classified improperly or unnecessarily.

Page I-15, paragraph 1-603a, Declassification and Downgrading Authority. Add the following to the subparagraph:

a. USEUCOM personnel identified in this supplement as having OCA may delegate declassification and downgrading authority to officials with technical knowledge of classified programs, projects and plans, provided such delegations are in writing and specify the information categories the official may act upon.

Table of Contents

Chapter II

CLASSIFICATION

Page II-2, paragraph 2-103b, Challenges to Classification. Add the following to the subparagraph:

b. Send challenges to classification of non-USEUCOM originated information through command channels to ECSM-SP. In other cases, send challenges to the security manager of the USEUCOM element or component originating the classified information. Use DA Form 1575 to make a formal challenge. Enter the rationale supporting the challenge in the "Remarks" section of the form. When it is probable that the originator may not be able to determine what document or material is being challenged, the challenger will include a copy of the document or material with DA Form 1575.

Page II-9, paragraph 2-405a, Distribution of Classification Guides. Add the following to the subparagraph:

a. Copies of each approved classification guide (less SCI) and changes will be forwarded to ECSM-SP for distribution to DoD and the Office of Industrial Security as appropriate. Originators also will furnish classification guides (or other classification guidance) to all probable users such as test and evaluation organizations or activities having an official and recurring interest in the subject matter.

Page II-14, paragraph 2-901, Contract Security Classification Specification. Add the following paragraphs and subparagraphs:

a. If classification considerations are simple (or brief), a

properly completed DD Form 254 will suffice.

b. Reviews will be made at the same time as reviews of associated security classification guides (see subsection 2-404).
Reviews of DD Form 254 will consider any difficulties or problems that have surfaced during use of the guidance and should
ensure that:

l. All classification guidance required by the contractor is provided.

2. The classification decisions involved have been
personally approved by an individual with the requisite classification authority.

3. The guidance is current and conforms with that found
in other sources.

4. The guidance is specific and unambiguous. Any problems encountered with interpretation of the guidance must be
carefully considered and resolved.

Page II-14, After Section 9, Industrial Operations, Add Section
10, Travel of Senior Officials, (Classification of General/Flag
Officer Itineraries) as follows:

a. Detailed itineraries of high risk targets (to include all
general/flag officers and civilian equivalents) will be marked at
least "For Official Use Only" when traveling anywhere within the
USEUCOM area of responsibility. When preparing and coordinating
itineraries, the office of primary responsibility for the high
risk target should review the threat and apply more stringent
controls to include classification IAW this directive on a case-
by-case basis as warranted. In all instances, particular attention should be given to OPSEC, and itineraries should be

protected to the maximum extent practicable by means of secure communications, personal contact, limited distribution and publicity avoidance. When warranted, public affairs offices may announce trips in advance, but press releases should not contain precise arrival/departure times and places. Only the composite, detailed itinerary which contains the overall schedule with arrival/departure times and places is classified when associated with the high risk target. Necessary coordination and administrative arrangements to develop and execute the itinerary may be handled as FOUO.

b. Itineraries will be classified Confidential and marked with the following classified by and declassify on lines when deemed necessary:

1. Classified By: USEUCOM Supplement 1 to DoD 5200.1-R

2. Declassify On: Upon completion of visit

Chapter IV - Marking

Table of Contents

Paragraph

CHAPTER IV

MARKING

Page IV-1, paragraph 4-101, Purpose of Designation. Add the following:

The holder of improperly marked classified documents must contact the document originator to obtain correct marking information. Particular care must be taken when reproducing classified documents to ensure that classification markings and associated markings are distinct and conspicuous on the reproduced copies. Documents will be remarked or stamped by hand to ensure legibility when markings are not clearly visible on reproduced copies.

Page IV-1, paragraph 4-102b, Exceptions. Add the following to the paragraph and add subparagraphs:

b. Use the following parenthetical symbols for documents which contain intelligence and NATO information IAW subsections 4-503 and 4-506.

1. Use "(OC)" for ORCON information.

2. Use "(PR)" for PROPIN information.

3. Use "(CTS)" for Cosmic Top Secret information.

4. Use "(CTSA)" for Cosmic Top Secret Atomal information.

5. Use "(NS)" for NATO Secret information.

6. Use "(NSA)" for NATO Secret Atomal information.

7. Use "(NCA)" for NATO Confidential Atomal information.

8. Use "(NR)" for NATO Restricted information.

Page IV-4, paragraph 4-200, Overall and Page Markings. Add the following subparagraph:

Documents twenty pages or less shall bear overall page markings commensurate to the highest level of classification assigned to the portion markings contained on that page.

Chapter V - Safekeeping and Storage

Table of Contents

CHAPTER V

SAFEKEEPING AND STORAGE

Page V-1, paragraph 5-100, General Policy. Add the following subparagraphs:

a. U.S. Missions will store and safeguard classified and administratively controlled materials in accordance with applicable regulations and policies of both the Department of State and the Department of Defense. At facilities approved for storage of classified information, the Regional Security Officer will designate controlled access areas and establish supervisory controls over the distribution and storage of classified and administratively controlled materials. All USEUCOM field element offices are subject to accreditation of classified storage areas by the Department of State.

b. DOD has agreed to comply with DOS minimum security standards. In those cases where DOD standards exceed DOS requirements, the DOD component office coordinates required upgrades with the DOS Regional Security Officer. If the Regional Security Officer and the Field Element Chief cannot agree on the level of upgrade, they will refer the disagreement through the Chief of Mission to the Department of State, and through Head-quarters United States European Command (ECJ4/ECSM-S) to the Defense Intelligence Agency in Washington, D.C. and request

resolution of the matter.

Page V-2, paragraph 5-102 Storage of Classified Information. Add the following paragraphs and subparagraphs:

e. Open Storage. Open storage will only be approved for material too large for containers; for bulk material that must be reviewed on a daily basis making storage in containers impractical; or for instances when classified containers are not available. Secure storage facilities for open storage of classified material will be established in accordance with the following:

1. Field elements located in facilities that fall under the jurisdiction of the Department of State will obtain DOS approval for open storage. Requests will be submitted IAW DOS procedures. All other HQ USEUCOM field elements will obtain HQ USEUCOM Chief of Staff approval for open storage. Requests will be submitted IAW Appendix K.

2. A memorandum designating the area as an open storage facility will be posted on or near the inside of the locking door to the facility. Facilities not possessing a memorandum of designation will contact ECSM-SP to determine what actions are necessary.

3. Open storage facilities must be reevaluated and recertified each time a structural change occurs to the open storage facility.

4. HQ USEUCOM Directorates which desire to store classified information in an open configuration will submit written requests to ECSM-SP for final approval. Include as a minimum justification, description of the type and quantity of material to be stored, and a statement identifying existing

physical security measures inherent to the storage facility. (See Appendix K.) Prior to submission of the written request for open storage to ECSM-SP, a physical security survey must be accomplished by the Provost Marshal's Office (PMO) to ensure the area meets the construction criteria for Class B vault, vault-type room, strong room, or secure storage room including an approved alarm system.

f. Storage Prohibitions.

1. Do not store funds, weapons, medical security items, controlled drugs, precious metals, or other items susceptible to theft, in any security type equipment, including vaults and vault-type rooms, which store classified material. HQ USEUCOM Chief of Staff may waive this requirement in emergencies, or temporarily when acceptable storage containers are not available.

2. Security equipment purchased for the use of storing classified material will not be used for routine storage of supplies and other nonadministrative unclassified material.

3. Security containers will not be used to solely store wholly unclassified material.

Page V-4, paragraph 5-104b1., Combinations to Containers. Add the following subparagraphs:

(f) Every 12 months when NATO information is stored in the security container.

(g) Persons having knowledge of combinations to containers containing NATO material will be NATO briefed.

Page V-6, paragraph 5-201, Care During Working Hours. Add the following subparagraphs:

d. Distinctively marked burn bags will be used for the collection of classified waste.

e. Custodial, maintenance, and construction personnel and all other uncleared personnel will be escorted at all times while in offices and controlled areas to prevent unauthorized access to classified material. Escorts will remain with custodial and uncleared personnel unless another responsible person accepts escort responsibilities. Elements are responsible for providing escorts in their own areas.

f. Classified material will not be carried loose when being handcarried between buildings. Such material will be carried in a folder or envelope or other suitable container not bearing classification markings.

g. Reversible "OPEN-CLOSED" or "OPEN-LOCKED" signs will be used on each security container in which classified information is stored.

Page V-6, paragraph 5-202, End of Day Security Checks. Add the following information, paragraphs, and subparagraphs:

A person discovering a security container or secure storage facility open and unattended will:

a. Keep the container or storage area under guard or surveillance.

b. Notify the element security manager and one of the persons listed on Part 1, SF 700, affixed to the inside of the container or storage area. If one of these people cannot be contacted, the duty officer or element chief will be notified.

c. The Security Manager or the individual contacted will:

1. Report personally to the location; check the contents of the container or area for visible indications of tampering, theft, or compromise. If any evidence of tampering, theft, or compromise is noted, installation or activity security personnel will be immediately notified so that an investigation can be initiated. The custodian will conduct an inventory of the container contents and report any discrepancies immediately.

2. When tampering is evident, the custodian will contact their Security Manager and ECSM-SP immediately. Do not touch until investigators have cleared the scene. Change the combination and lock the container as soon as possible, once the investigative offices have completed their assessment. If the combination cannot be changed immediately, the security container will be secured and placed under guard until the combination can be changed, or the classified contents will be transferred to another security container or secure area.

3. Report the incident to ECSM-SP within 24 hours or the next duty day.

Page V-10, paragraph 5-203, Emergency Planning. Add the following subparagraphs:

m. Emergency plans will be labeled "For Official Use Only." The plan will be filed as the first document in the locking drawer of each security container or in an area deemed appropriate by the security manager.

n. Elements will conduct, at a minimum, semiannual drills to determine the adequacy of emergency plans. A record of these drills will be maintained by the element security manager.

Page V-10, paragraph 5-205, Security of Meetings and Conferences.

In order to ensure compliance with the appropriate regulations, ECSM-SP will be notified immediately of plans to
conduct classified meetings and conferences.

Chapter VI - Compromise of Classified Information

Table of Contents

Discoverer

6-103 Preliminary Inquiry

CHAPTER VI

COMPROMISE OF CLASSIFIED INFORMATION

Page VI-1, paragraph 6-100, Policy. Add the following:

Field element offices located at Department of State facilities will, in addition to this Supplement, follow the security violations reporting procedures established in Department of State regulations and policies.

Page VI-1, paragraph 6-102, Responsibility of Discoverer. Add the following to the subparagraph:

a. Additionally, report this information to HQ USEUCOM (ECSM-SP) within 24 hours or the next duty day.

Page VI-1, paragraph 6-103, Preliminary Inquiry. Add the following to the introductory paragraph:

The preliminary inquiry must follow the format in Appendix I and be initialed by the staff element director or chief to indicate concurrence with the recommendations and corrective actions as stated in the preliminary inquiry. Additionally, this report must be submitted to HQ USEUCOM (ECSM-SP) within ten working days after the initial 24 hour notification to HQ USEUCOM. If during the conduct of an inquiry it is discovered that the possibility of espionage, subversion or deliberate acts of compromise were involved in the violation, immediate notification will be made to HQ USEUCOM (ECSM-SP).

Chapter VII - Access, Dissemination, and Accountability

Table of Contents

CHAPTER VII

ACCESS, DISSEMINATION, AND ACCOUNTABILITY

Page VII-6, paragraph 7-205, NATO Information. Add the following subparagraphs:

a. NATO Atomal documents will be controlled on HQ USEUCOM Form 23a, Atomal Register.

b. NATO Cosmic Top Secret documents will be controlled on HQ USEUCOM Form 23b, Cosmic Top Secret Register.

c. NATO Secret documents will be controlled on HQ USEUCOM Form 24, NATO Secret Register.

d. NATO Secret, Cosmic and Atomal information will be inventoried in the same manner prescribed in paragraph 7-300c.

e. Removable ADP media (diskettes or cartridges) containing NATO information will be accounted for on the appropriate HQ USEUCOM Forms 23a, 23b, and 24, commensurate to the level of classified information contained on the media.

Page VII-8, paragraph 7-300a, Control Officers. Add the following to the paragraph and add subparagraphs:

a. TSCO will at a minimum:

1. Maintain a Top Secret Register.

2. Receive, sign for, and dispatch all Top Secret material transmitted to or from the elements they serve; and maintain receipt for Top Secret material dispatched or transferred.

3. Conduct periodic checks within the element to ensure the proper handling and safeguarding of Top Secret information.

4. Monitor the reproduction of Top Secret material.

5. Ensure persons having custody of Top Secret material are properly relieved of accountability before they depart on leave or temporary duty for more than 45 days, or when they are transferred, reassigned, separated, retired, or otherwise change status with regard to custody or possession of Top Secret material.

6. Report any action or omission by personnel which violates rules for safeguarding and controlling Top Secret information to the element chief or element security manager and ECJ1-SP.

Page VII-8, paragraph 7-300b, Accountability, 1. Add the following to paragraph 1 and add the following subparagraphs.

1. Top Secret material, including removable ADP Media (diskettes and cartridges), will be accounted for on USEUCOM Form 23, Top Secret Register.

(e) Assign a consecutive number to each register by including the calendar year and TSCA functional address symbol; for example: 91-ECJ1-0043. Use the alphabetical letter A,B,C and so on to prepare continuation pages to the basic form.

(f) Each register will remain active until it is made inactive; for example: transferring material to another TSCO; destroying the material; posting entries to; or incorporating with another recorded document; or downgrading and/or declassifying based on proper authority.

(g) Inactive registers will be maintained on file for five years.

Page VII-8, paragraph 7-300b, Accountability, 3. Disclosure Records. Add the following to the subparagraph.

3. Attach AF Form 144, Top Secret Access Record and Cover Sheet, to each Top Secret document or material including removable ADP Media (diskettes or cartridges) to identify all persons given access to the information. AF Form 144 will be kept with the document at all times until the document is destroyed, transferred to another TSCO, downgraded, or declassified. Once action has been taken as mentioned above, attach AF Form 144 to the inactive USEUCOM Form 23 and maintain on file for five years.

Page VII-9, paragraph 7-300c, Inventories. Add the following to the subparagraph.

c. Additionally, inventories will be conducted on change of the TSCO or whenever directed by the TSCO appointing authority. The TSCO will not perform the inventory.

Page VII-10, paragraph 7-301b, Secret Information. Add the following to the subparagraph.

b. When Secret material is being transmitted outside of the Command a DA Form 3964, Classified Document Accountability Record will be used to record its receipt and dispatch.

Chapter VIII - Transmission

Table of Contents

8-202b Receipt Systems

8-303b Authority to Approve or Escort Handcarrying of Classified Information Aboard Commercial Aircraft

8-304 (a,b,c) Authorization for Escorting or Handcarrying Classified Material

CHAPTER VIII

TRANSMISSION

Page VIII-1, paragraph 8-101b, Top Secret Information. Add the following to the subparagraph:

b. Within USEUCOM, the USEUCOM Courier will provide this service.

Page VIII-10, paragraph 8-202a, Receipt Systems. Add the following to the subparagraph:

a. Top Secret Register Pages may be used as a receipt when transferring Top Secret material from one TSCA to another on the same installation. This applies to releasing Top Secret messages and computer input data products to telecommunications facilities, data processing installations, and data processing centers for secondary transmission or data processing.

Page VIII-10, paragraph 8-202b Receipt Systems. Add the following to the subparagraph:

b. Use a receipt when entering Secret material into a mail distribution system, secondary distribution systems, or the US Postal Service.

Page VIII-15, paragraph 8-303b, Authority to Approve or Escort Handcarrying of Classified Information Aboard Commercial Passenger Aircraft. Add the following to the subparagraph:

b. HQ USEUCOM Directors/Office Chiefs and in their absence, Deputies are authorized to approve the handcarrying of classified aboard commercial aircraft.

Page VIII-15, add paragraph 8-304, Authorization for Escorting or Handcarrying Classified Material. The paragraphs (a-c) should read as follows:

a. All USEUCOM personnel escorting or handcarrying classified outside their normal work area require authorization for such action. Also, these personnel will use an envelope, briefcase, or other closed container to prevent loss or

observation of classified material being handcarried outside work areas. A verbal approval from the individual's supervisor is sufficient when handcarrying between buildings or areas where the travel does not pass through a known or probable site of a DoD inspection point (gates to the installation, entries to facilities controlled by guards and so forth).

b. When classified materials are transported between installations or equivalent organizations written authorization is required. Written authorization may be either an official letter or a DD Form 2501, Courier Authorization Card (this is a 3 1/4 X 4 1/4 inch card), signed by the director, field element chief, or their appointed designee. Individuals authorized to escort or handcarry classified material will receive a security briefing covering the contents of DoD 5200.1-R, Chapter VIII. (See Appendix J.)

c. Personnel handcarrying classified information aboard Government or Commercial Aircraft will comply with the provisions listed in paragraphs 8-300, 8-301, and 8-302.

Chapter IX - Disposal and Destruction

Table of Contents

CHAPTER IX

DISPOSAL AND DESTRUCTION

Page IX-1, paragraph 9-101, Methods of Destruction. Add the following:

An aggressive downgrading and destruction program contributes to effective emergency planning. USEUCOM elements will review at least 25 percent (or 3 linear feet, whichever is more) of classified holdings each quarter to determine whether or not the material may be destroyed, declassified, or downgraded. Standards for commonly used destruction equipment are identified at Appendix G.

Page IX-2, paragraph 9-105, Classified Document Retention. Add the following subparagraphs:

c. The first Wednesday in February is the HQ USEUCOM annual clean-out day.

d. A quarterly purge of classified holdings will be conducted.

Chapter X - Security Education

Table of Contents

10-106 (a,b,c,d) Other Briefing Requirements

CHAPTER X

SECURITY EDUCATION

Page X-1, paragraph 10-100, Responsibility and Objectives. Add the following subparagraphs:

a. Security Education training is done in two phases: Indoctrination and Recurring training.

b. Information security indoctrination and recurring training, as a minimum, will include all subject areas listed in paragraph 10-101 of DOD 5200.1-R. USEUCOM element chiefs will ensure indoctrination and recurring training programs are established and conducted properly.

c. Indoctrination training will be conducted within 30 days of an individual's arrival at USEUCOM elements. For those members arriving on temporary duty (TDY) assignments, the host element chief provides indoctrination training as required by the specific mission of the TDY. Recurring training will be conducted at a minimum annually.

d. Records of all security education training will be maintained by the element security manager. Records will include: target audience, date training was conducted, and subjects presented.

Page X-3, add paragraph 10-106, Additional Briefing Requirements.
It should read as follows:

The following Special Briefings are required to be conducted:

a. When an employee is authorized to carry or escort classified material (see paragraph 8-300f).

b. When an employee is granted access to Sensitive Compartmented Information or information subject to special access program controls (if the program so requires).

c. When an employee is granted access to NATO classified information.

d. Biennial requirements for counterintelligence briefings will be coordinated with local Military Intelligence units. Field elements located at DoS locations should coordinate these briefings with the Regional Security Officer.

Chapter XII - Special Access Programs

Table of Contents

CHAPTER XII

SPECIAL ACCESS PROGRAMS

Page XII-2, paragraph 12-101e, Establishment of Special Access Programs. Add the following to the paragraph and add subparagraphs:

e. A USEUCOM activity planning to establish a Special Access Program, or to participate in a program directed by another DoD Component must send a recommendation for establishment or participation through command channels to ECSM-SP. The request must contain the information identified in DoD 5200.1R, Chapter XII, Paragraph 12-105a. ECSM-SP reviews the recommendation and takes the following action:

1. Forwards the request to the Chief of Staff for concurrence and ensures the request is submitted to DUSD(P) for approval.

2. Returns all Chief of Staff nonconcurrences to the recommending activity.

Page XII-2, paragraph 12-102a, Review of Special Access Programs. Add the following to the subparagraph:

a. The Special Access Program Manager of each approved USEUCOM program will ensure the conduct of annual reviews and document these reviews each December.

Page XII-3, paragraph 12-103, Control and Central Office Administration. Add the following subparagraph:

c. HQ USEUCOM Security Manager, ECSM-SP, is the central point of contact for all USEUCOM Special Access Programs, except SCI programs which are under the control of ECJ2-SSO. ECSM-SP will maintain a listing of all HQ USEUCOM Special Access Program Focal Point Officers and program nicknames. The ECSM-SP Special Access Program (SAP) list will be updated annually.

Page XII-4, paragraph 12-105c, Termination Reports. Add the following to the subparagraph:

c. The Special Access Program Manager responsible for the approved Special Access Program sends SAP termination reports to ECSM-SP as required. ECSM-SP will forward report to The Deputy Under Secretary of Defense for Policy (DUSDP).

Paragraph XII-6, paragraph 12-108, "Carve Out" Contracts. Add the following subparagraph.

g. USEUCOM elements sponsoring a Special Access Program affecting a contractor will use DD Form 254 as the legally binding instrument. ECSM-SP will be provided one copy of the completed DD Form 254 for submission to the Director, DIS.

Chapter XIII - Program Management

Table of Contents

CHAPTER XIII

PROGRAM MANAGEMENT

APPENDIX F

ORIGINAL SECRET CLASSIFICATION AUTHORITIES

(See paragraph 1-600b3)

The USEUCOM officials identified below are authorized to make original classification authority determinations for information up to and including SECRET.

Director, Manpower, Personnel and Security Directorate (ECJ1)

Director, Intelligence Directorate (ECJ2)

Director, Operations Directorate (ECJ3)

Director, Logistics & Security Assistance Directorate (ECJ4)

Director, Plans and Policy Directorate (ECJ5)

Director, Command, Control, and Communications Systems Directorate (ECJ6)

Special Assistant for Security Matters (ECSM)

Director, Office of Analysis and Simulation (ECCS-AS)

Director, Comptroller (ECCM)

Director, Inspector General (ECIG)

Director, Public Affairs (ECPA)

Director, Special Operations Directorate (ECSO)

Legal Advisor (ECLA)

Command Surgeon (ECMD)

Command Chaplain (ECCH)

Chief, Joint Analysis Center (JAC)

Chief, USNMR, SHAPE

Chiefs of Field Elements to include ODCs, SAOs, etc...

APPENDIX G

CLASSIFIED MATERIAL DESTRUCTION STANDARDS

(See paragraph 9-101)

1. General. This appendix contains basic concepts and guidelines that assist in determining the sufficiency of various destruction techniques. It also provides residue dimension standards that will assist in achieving secure destruction. No single destruction method has been found to be as effective, versatile, and secure as burning.

2. The methods for routine destruction of classified material shown below are approved for use by USEUCOM elements.

a. Pyrolysis (high temperature multistage).

b. Shredding.

c. Pulping (wet process).

d. Pulverizing (dry process).

3. Approved routine security destruction equipment.

a. Design specifications of equipment used for each of the destruction methods in paragraph K-3 will, as a minimum, conform to the following applicable standards:

(1) Pyrolytic furnaces - Federal Clean Air Act, as amended.

(2) Shredders - Interim Federal Specifications FF-S-001169 with amendment 3.

(3) Pulping Machines - Interim Federal Specifications FF-P-00800A with amendment 2.

(4) Pulverizing Machine - Interim Federal Specifications FF-P-00810A with amendment 3.

(5) All others - to be approved by Intelligence Materiel Development and Support Office (IMDSO) per paragraph 9-101 prior to procurement.

b. Residue Standards.

(1) Pyrolysis. Pyrolytic furnace ash residue must not contain unburned product. If unburned product is found, it will be treated as classified waste and maintenance personnel will be instructed to correct this fault in the furnace's burn cycle. Ash residue is to be examined and reduced by physical disturbance and will be considered destroyed when capable of passing through a 1/2 inch (13mm) square wire sieve. Furnace operators should be

permanently assigned and trained to perform necessary adjustments and maintenance and be cleared for access to the highest level of material being routinely destroyed.

(2) Shredders. The Class I shredder identified by GSA Interim Federal Specifications FF-S-001169 as producing a residue measuring 1/32 inch + 1/64 inch tolerance by 1/2 inch crosscut is approved for destruction in "secure volume" of up to Top Secret material. Any crosscut shredder whose residue particle size (total area) is equal to or smaller than that of the above Class I shredder (15.12mm2 or 0.02344in2) is similarly approved for Top Secret destruction, when used in accordance with the "secure volume" concept of operation. Classified microfilm, microfiche, or similar high data density material will not be destroyed by shredding.

(3) Pulping. The Interim Federal Specifications FF-P-00800A with amendment 2 specifies the perforated screen or ring used in the masticating unit (through which all pulp must pass) will have 1/4 inch (6.350mm) or smaller diameter perforations. Since the pulping process entails wetting and dissolving action, plastic-based or other water-repellent-type papers normally should not be put through this system. However, if wetting additives are used and the ratio of soluble to nonsoluble paper kept high (16 to 1 or greater), the masticating unit normally will tolerate that material. This toleration is totally dependent upon the sharpness of the pulper's cutters. Foreign matter, such as metal and glass, must be excluded from charge loads by visual inspections. Standard systems employing 1/4 inch diameter perforated security screen are approved for the

destruction of classified paper-based documents through Top Secret. Top Secret material will not be destroyed on equipment where security screens with larger perforations are in use. Random samples of residue from such units should be collected by the security manager for periodic examination. Samples may be sent to IMDSO for evaluation and comment.

(4) Pulverizers. The Interim Federal Specifications FF-P-00810A with amendment 3 covers pulverizing as a dry destruction process. It does not, however, specify a specific dry destruction method; consequently, within this category are hammer mills, choppers, hoggers, and hybridized disintegrating equipment.

APPENDIX I

SAMPLE PRELIMINARY INQUIRY REPORT MEMORANDUM

(See paragraph 6-103)

ECJX-XX

MEMORANDUM THRU DIRECTOR (Of element submitting the inquiry)

FOR ECSM

SUBJECT: Preliminary Inquiry - Control No. EC-96-1

1. Reference. DoD 5200.1-R, Information Security Program Regulation, and the HQ USEUCOM Supplement.

2. Authority. A preliminary inquiry was conducted from 21 through 23 Mar 96 under the authority of the above reference.

3. Description of Incident: The basis for this inquiry was that a Secret message was found unsecured in Room 248 of Building 3322 at approximately 1240 hours, 20 Mar 96.

4. Personnel Interviewed:

a. MSgt John P. Smith, ECJX-XX.

b. Capt Bill Jones, Joint Staff J1.

c. SSgt Larry Williams, ECJX-XX.

d. Maj Roger Moore, ECJX-XX.

5. Facts. Testimony provided to and observations of the inquiring official revealed:

a. A Secret message, reference 1.c., was transmitted from ECJX-XX to ECJX-XX on 19 Mar 96. According to Capt Jones, the message was transmitted as priority precedence in the support of the Stilwell Commission.

b. At approximately 1130, 20 Mar 96, SSgt Williams received a telephone call from the Vaihingen Telecommunications Center (VTCC) about the reference Secret message. Notification of classified message pick-ups is a routine action between the VTCC and ECSM. SSgt Williams proceeded to the VTCC and took possession of the referenced Secret message.

c. Upon SSgt Williams' return to his work place at approximately 1150, 20 Mar 96, SSgt Williams processed the message and noted that the message was for immediate action by the ECJX-XX office. SSgt Williams handcarried the message to the ECJX-XX branch. The message was left in the "in basket" and SSgt Williams left the building for a racquetball appointment.

d. The message was found unsecured at approximately 1249, 20 Mar 96 by MSgt Smith upon his return from his scheduled lunch. The message was under a stack of paper in the "in basket." MSgt Smith did not recall receiving the message prior to going to

lunch.

e. The ECJX-XX office area is not a secured area. There are three individuals, all with Secret security clearances, that work in the area. Very little public traffic occurs in the area of the ECSM-SP office. Although the facility receives contract janitorial services, the cleaning crew normally cleans the room around 1400 each duty day. Maj Moore, who occupies the adjacent office, did not recall seeing any personnel in the ECJX-XX office during the time period the message was left unsecured.

6. Conclusion. As a result of the testimony and of personal observations, it is concluded that:

a. The incident occurred by unit personnel failing to follow established safeguarding procedures. Operating instructions direct the "hand-to-hand" release/transfer of classified material and prohibit use of in baskets.

b. SSgt Williams' haste to meet a scheduled racquetball appointment caused a variance in protection procedures.

c. The message was left unsecured for approximately 40 minutes. There is no evidence that unauthorized personnel had access to the message.

d. A compromise of classified information did not occur.

7. Recommendations. Recommend that:

a. Additional emphasis on unit procedures be addressed at regular intervals to enhance unit security education.

b. That this incident should be closed as a security deviation.

Encl THEODORE W. MATTESON
Interview Statements Major, USAF
Inquiry Official

Figure I-1. Continued.

Instructions for Completing a Preliminary Inquiry Report

Report Content. Up to this point, you have made a determination of facts by checking records, reviewing directives, examining evidence, and interviewing people. It is now time to sit down and write the report. To assist you in preparing the written report, it is important to understand the general content for each of the seven sections of the written report. The follo-wing explanation of each of the sections is provided.

a. Section I - References. This paragraph is used to reference any applicable directives, the authority for the inquiry, and any other documents which are referenced in the inquiry report.

b. Section II - Authority. This paragraph of the report cites the authority for conducting the inquiry and states when, where, and by whom the inquiry was conducted.

c. Section III - Matters Investigated. This paragraph contains a brief statement of the matter inquired into, the location of the security incident, and how the security incident was initially discovered or reported. When names of personnel are included, furnish their full name, rank, and duty title.

d. Section IV - Personnel Interviewed. List all personnel who were interviewed by showing their rank, full name, duty title or functional address.

e. Section V - Facts. This section is the heart of the entire inquiry report. It presents, in an orderly fashion, all established facts which have a bearing on the security incident. Facts are presented in chronological order with opinions and evaluation being omitted.

f. Section VI - Conclusion. This section will contain a brief summary of conclusions reached after a review of all pertinent information by the inquiry official. Conclusions must be supported by the evidence obtained during the inquiry process. One of the following must be established: (1) compromise occurred; (2) possible compromise occurred; (3) inadvertent access occurred; or (4) the incident is a security deviation. One of the most important tasks of an inquiry official is to ascertain who or what is responsible for the security incident. The job is not finished unless this is accomplished and documented. Occasionally, there is a systemic or procedural breakdown where an activity fails to properly safeguard classified material due to misunderstanding of a requirement or, even more rarely , disregarding or ignoring requirements and lack of an effective security education and training program. Whatever the situation, the person or procedure that caused the incident is identified so corrective and preventive action can be taken by the appointing official.

g. Section VII - Recommendations. This last section contains the inquiry official's recommendations for further action. Based on the conclusion (section V of the report, you
can recommend the incident be deemed a security deviation and the
incident closed. A recommendation on the need for an investigation is necessary when it has been

APPENDIX J

SAMPLE COURIER AUTHORIZATION MEMORANDUM AND EXEMPTION NOTICE

(See paragraph 8-302d1(c))

ECJX

MEMORANDUM FOR Whom It May Concern

SUBJECT: Designation of Official Courier

1. Major John Smith, SSN 123-45-6789, XXXXXXXXXXXXX Directorate (ECJX), HQ U.S. European Command, APO AE 09128, is designated an official courier for the United States Government. Upon request, he will present his official identification card bearing the number A-1111222.

2. Major Smith is handcarrying three sealed packages, size 9" x 8" x 24" addressed from "HQ USEUCOM, ATTN: ECJX-XX, APO, AE 09128-4209," and addressed to "DoD Historian, The Pentagon, Room 3C333, Washington, DC 20330-4000." Each package is identified on the outside of the package by the marking "OFFICIAL BUSINESS - MATERIAL EXEMPTED FROM EXAMINATION" bearing the signature of the undersigned.

3. Major Smith is departing Stuttgart International Airport, Germany with a final destination to Washington National Airport, District of Columbia. Known transfer points are Frankfurt International Airport, Germany and John F. Kennedy International Airport, New York.

4. This courier designation can be confirmed by contacting the undersigned at HQ USEUCOM ECJX, 49-711-680-9988 (U.S. to overseas); 0711-680-9988 (overseas to overseas); or DSN 430-9988.

JOHN J. BIGBOSS
Brigadier General, USA
Director,

_____

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400, BOX 1000
APO AE 09128-4209

Change 1 to
USEUCOM SUP 1
to DOD 5200.1-R 30 March 1998

Information Security Program

Policy and Procedures for the development of information security programs in USEUCOM.

USEUCOM Sup 1 to DOD 5200.1-R, 29 Oct 97, is changed as follows:

Pen-and-ink changes:

a. Page 4, chapter 1, paragraph 1-301, SCI & COMSEC; change: ECJ2-Site Security Officer to **Special** Security Officer.

b. Page 7, chapter 2, para 2-201, Delegation of Authority; change: Appendix F to Appendix **L**.

c. Page 9, chapter 4, para 4-102(f), Declassification and Downgrading Authority; change: Appendix S to Appendix **Q**.

d. Page 24, chapter 6, para 6-402(g)(4), Storage of Classified Information; change:
Appendix K to Appendix **P**.

e. Page 25, chapter 6, para 6-404, Combinations to Containers; Add the following para: 6-404(a) **Interiors of each security container drawer, vault or storage room will be marked with numeric 1, 2 and 3 stickers to indicate the priority of its contents for destruction. Within SCIF facilities, these stickers may be placed on the outside of security containers**.

f. Page 34, chapter 9, para 9-100, General Policy: Add: **(5) Individuals appointed to the position of Security manager will submit an appointment letter to HQ USEUCOM, Special Assistant for Security Matters (ECSM). Individuals will attend the HQ USEUCOM Security Managers Course within 6 months of appointment.**

g. Page 35, chapter 9, para 9-303, Derivative Classifiers, Security Personnel and others; change: l. Appointed Security Managers will: to **k**. Appointed Security Managers will:

Change 1 to
USEUCOM SUP 1
to DOD 5200.1-R

Information Security Program

h. Appendix J, page J-4, para g(4), change to read: NATO Secret, Cosmic and Atomal information will be accounted for and inventoried in the same manner as U.S. Top Secret, Appendix J, para 4 (1) and in accordance with USSAN 1-69.

I. Appendix Q, Declassification and Downgrading Authorities. Delete all ECJ4 “Chief” entries and replace with the following:

Chief, Military Secretariat - Secret
Chief, Logistics Operations Division - Secret
Chief, Logistics Plans Division - Secret
Chief, Joint Movement Division - Secret
Chief, Engineering Division - Secret
Chief, Multinational Agreements Division - Secret
Chief, International Division - Secret
Chief, Program and Policy Division - Secret

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

DAVID L. BENTON III
Lieutenant General, USA
Chief of Staff

SUSAN M. MEYER
LTC, USA
Adjutant General

DISTRIBUTION:

P

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400, BOX 1000
APO AE 09128-4209

Change 2 to
USEUCOM SUP 1
to DOD 5200.1-R 11 May 1998

Information Security Program

Policy and Procedures for the development of information security programs in USEUCOM.

Make the following Pen and Ink changes to USEUCOM Sup 1 to DOD 5200.1-R, 29 Oct 97.

a. Page J-2, Appendix J, paragraph b.1(a)(6); change 5 years to 2 years.

b. Page J-2, Appendix J, paragraph b.1(a)(7); change 5 years to 2 years.

c. Page J-3, Appendix J, paragraph c.1 and c.2; change 5 years to 2 years.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

DAVID L. BENTON III
Lieutenant General, USA
Chief of Staff

SUSAN M. MEYER
LTC, USA
Adjutant General

DISTRIBUTION:
P